RSAC 2025 Conference

Many Voices. One Community.

SESSION ID: GRC-M02

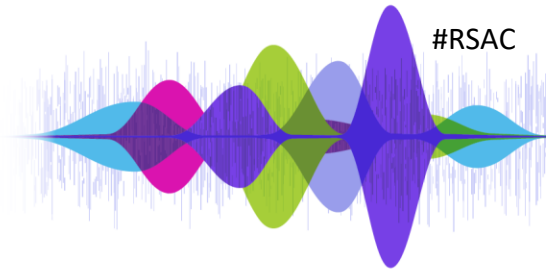
Somebody's Responsibility is Nobody's Responsibility: SRMs for the Win!

Lawrence Cruciana, CISSP, CISM, CISA, GCCC, CCP

President
Corporate Information Technologies
https://www.linkedin.com/in/lawrence-cruciana/

Matt Lee, CISSP, CCSP, CCSK, CCZT, CFR, PNPT

Security and Compliance Senior Director
Pax8
https://www.linkedin.com/in/cybermattlee/



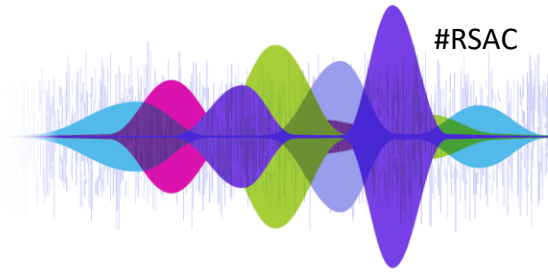
Disclaimer

Presentations are intended for educational purposes only and do not replace independent professional judgment. Statements of fact and opinions expressed are those of the presenters individually and, unless expressly stated to the contrary, are not the opinion or position of RSA Conference LLC or any other co-sponsors. RSA Conference LLC does not endorse or approve, and assumes no responsibility for, the content, accuracy or completeness of the information presented.

Attendees should note that sessions may be audio- or video-recorded and may be published in various media, including print, audio and video formats without further notice. The presentation template and any media capture are subject to copyright protection.

© 2025 RSA Conference LLC or its affiliates. The RSAC and RSAC CONFERENCE logos and other trademarks are proprietary. All rights reserved.

Introductions



Matt Lee

Lawrence Cruciana

Key Points

- Information flow (and thus responsibility) in modern business is complex
- IT is a team sport, clear rules are necessary
- Don't Assume, be clear
- SRMs A.N.C.H.O.R the service relationship

Setting it up

- We're going to make lots of references to the CIS Controls

  (Sorry, not sorry)

- We hope this presentation makes you productively uncomfortable

https://www.corp-infotech.com/ciscontrols

Setting it up

- Want to play along at home?...

https://www.corp-infotech.com/rsac25

Downloadable Kill Chain and reference information

Sodinokibi

REVIL

IDENTITY & ACCESS

Target HVAC Contractor Says It Was Breached By Hackers

A contractor that provides HVAC (heating, ventilation, and air conditioning) services for Target Corp. said on Thursday that like Target, it too was a victim of a sophisticated cyber attack.

By Mike Lennon
February 7, 2014

KrebsonSecurity
In-depth security news and investigation

Target Hackers Broke in Via HVAC Company

February 5, 2014 268 Comments

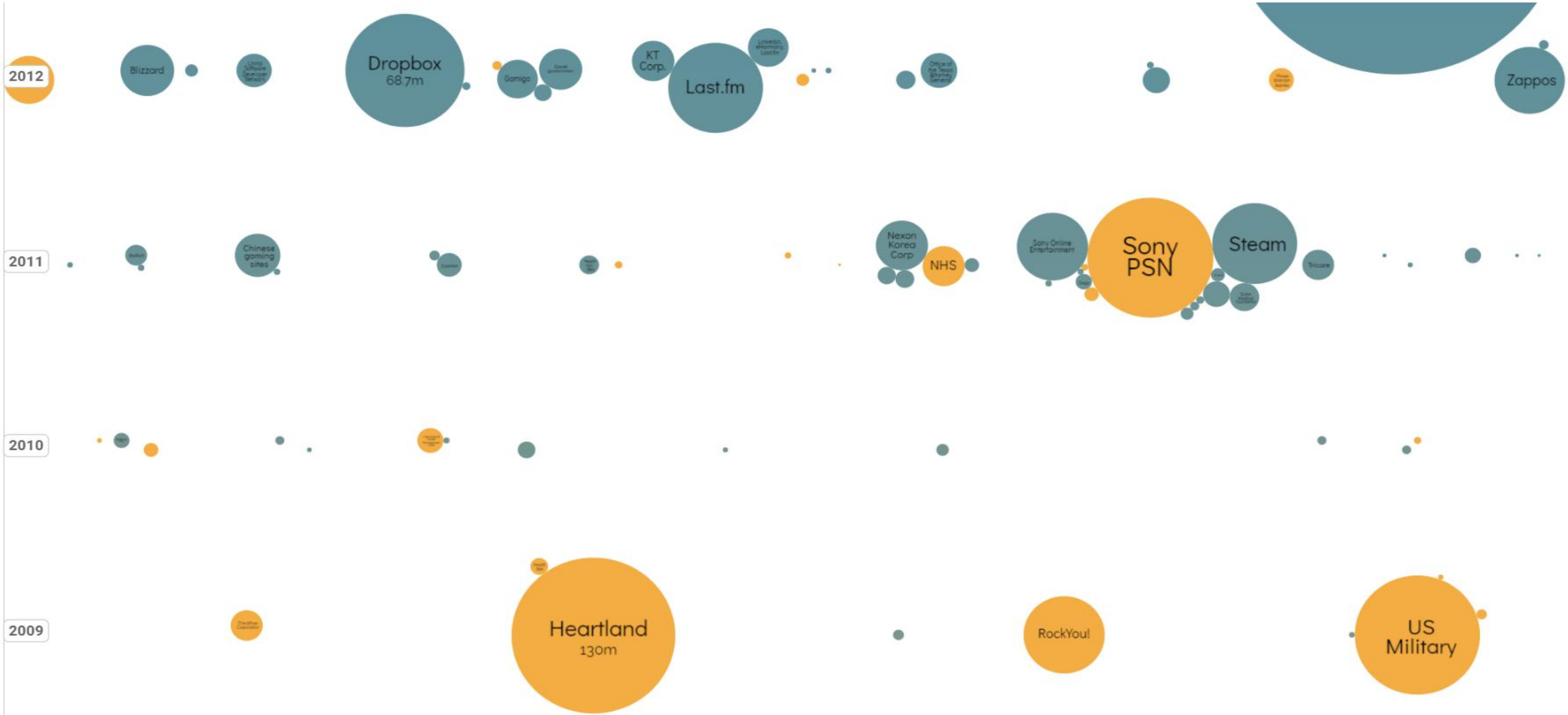
Last week, **Target** told reporters at *The Wall Street Journal* and *Reuters* that the initial intrusion into its systems was traced back to network credentials that were stolen from a third party vendor. Sources now tell KrebsOnSecurity that the vendor in question was a refrigeration, heating and air conditioning subcontractor that has worked at a number of locations at Target and other top retailers.

Sources close to the investigation said the attackers first broke into the retailer's network on Nov. 15, 2013 using network credentials stolen from Fazio Mechanical Services, a Sharpsburg, Penn.-based provider of refrigeration and HVAC systems.

Fazio president Ross Fazio confirmed that the **U.S. Secret Service** visited his company's offices in connection with the Target investigation, but said he was not present when the visit occurred. Fazio Vice President **Daniel Mitsch** declined to answer questions about the visit. According to the company's homepage, Fazio Mechanical also has done refrigeration and HVAC projects for specific Trader Joe's, Whole Foods and BJ's Wholesale Club locations in Pennsylvania, Maryland, Ohio, Virginia and West Virginia.

World's Biggest Data Breaches & Hacks

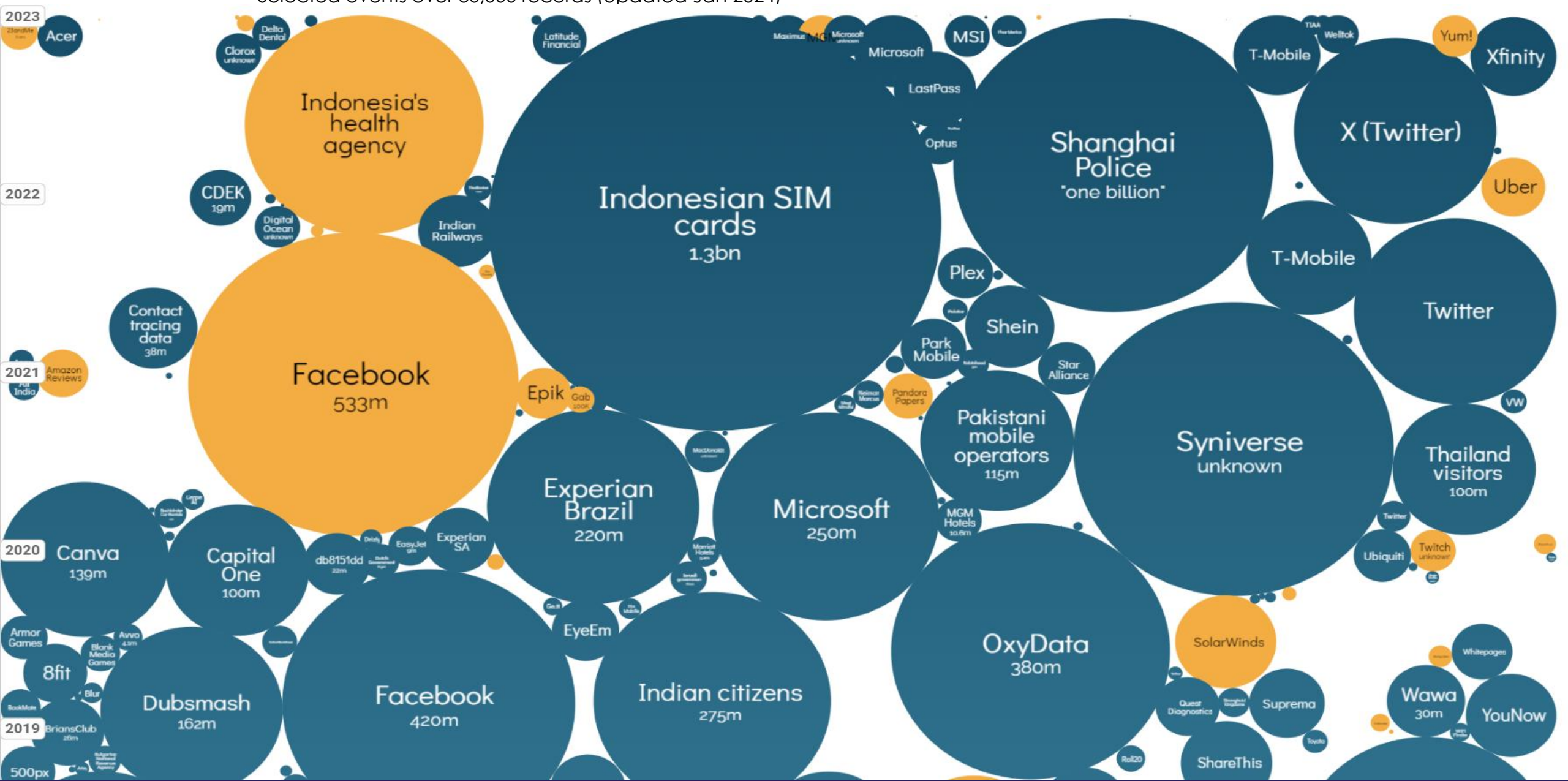
Selected events over 30,000 records (Updated Jan 2024)



Source: Information is Beautiful, Data visualization of the world's biggest data breaches and hacks, Jan 2024

World's Biggest Data Breaches & Hacks

Selected events over 30,000 records (Updated Jan 2024)



Small Business Data Center

Learn about small businesses' contributions to the economy and the unique challenges they face.

Stephanie Ferguson
Director, Global Employment Policy & Special Initiatives, U.S. Chamber of Commerce

Isabella Lucy
Graphic Designer, U.S. Chamber of Commerce

Published
May 25, 2023

46% of Businesses

Small business drives the U.S. economy. Small businesses employ nearly half of the entire American workforce and represent 43.5% of America's GDP. They are a critical part of our economic ecosystem where big businesses and small businesses are vendors, employees, partners, and customers to each other.

This data center includes facts, statistics and data visualizations about small businesses' contributions to the economy and the unique challenges that Main Street businesses face.

Small businesses fuel the economy.

How do SMB's deal with security?

The SMB Market Represents 44% Of All Tech Spend And Is 80% Partner-Delivered

Jay McBain
Chief Analyst - Channels, Partnerships & Ecosystems - Canalys - Channel Influencer of the Year

109 articles ✓ Following

September 13, 2023

GrrCON

Noon	**story-time with atlas (with hex)** – Atlas of D00m
1:00	**MSP's suck, but the world without them is worse** – Jason Slagle and Matt Lee
2:00 PM	**Boats are scary** – Arron Finnon
3:00 PM	**Shining a light into the security blackhole of IoT and OT** – Huxley Barbee (void *)
3:30 PM	**PCI DSS v4.0 Is Here – Now What?** – Kyle Hinterberg
4:00 PM	**Recalling early Unix System development at AT&T Bell Labs** – Richard Haight

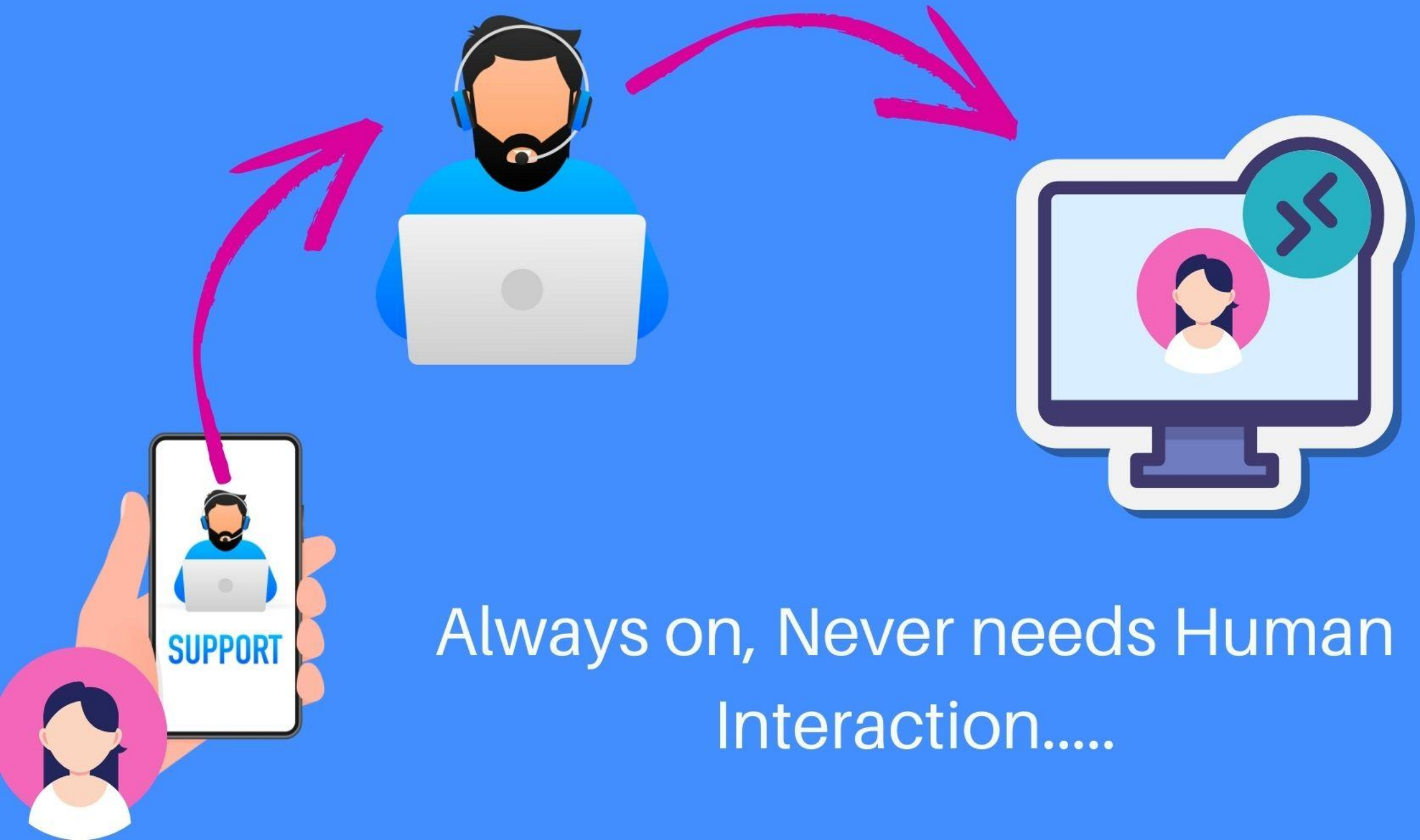
Counts by Annual Sales (Updated 2023-03-30)

Annual Sales Ranges	Number of Businesses
Under 500,000	14,382,087
500,000 - 999,999	818,345
1,000,000 - 2,499,999	559,315
2,500,000 - 4,999,999	226,121
5,000,000 - 9,999,999	148,583
10,000,000 - 99,999,999	181,386
100,000,000 - 499,999,999	24,708
500,000,000 - 999,999,999	4,174
1,000,000,000+	5,334
Uncoded records	1,882,514
Grand Total	18,232,567

6-7% TOPLINE REVENUE FOR TECH ON AVERAGE

- 98% OF COMPANIES HAVE <100 EMPLOYEES
- 89% <20 EMPLOYEES
- WHAT WOULD THOSE COMPANIES DO FOR IT?

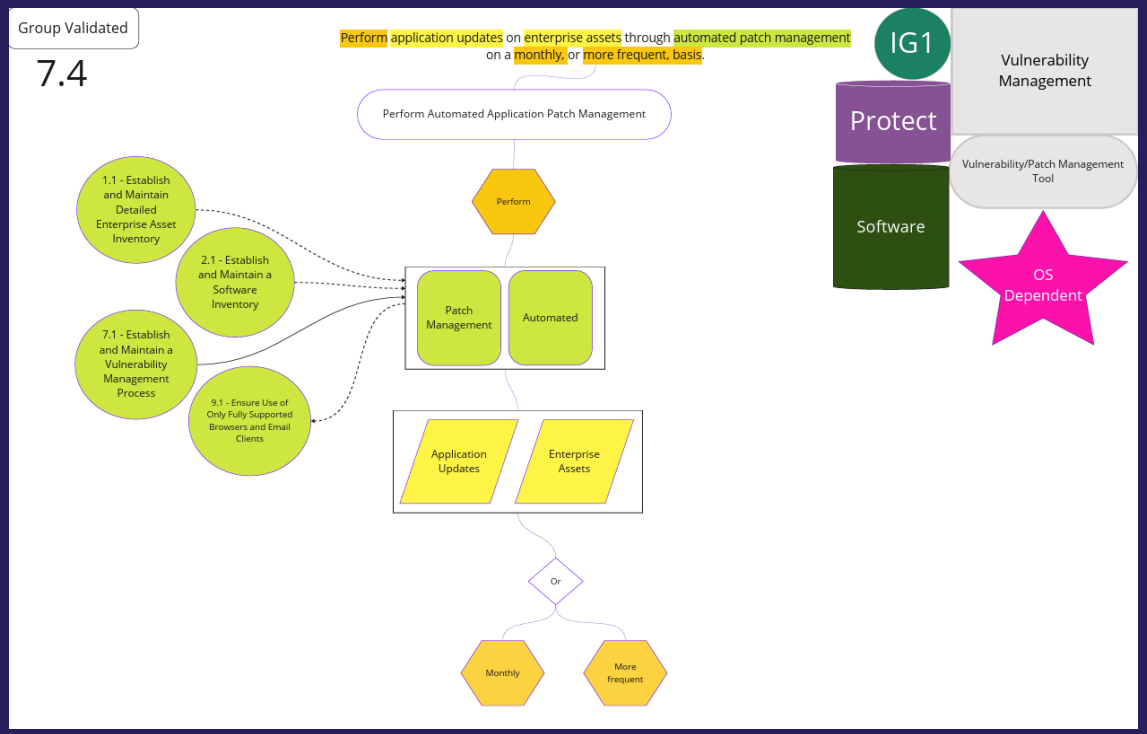
https://avasant.com/report/it-spending-as-a-percentage-of-revenue-by-industry-company-size-and-region/
https://www.naics.com/business-lists/counts-by-company-size/

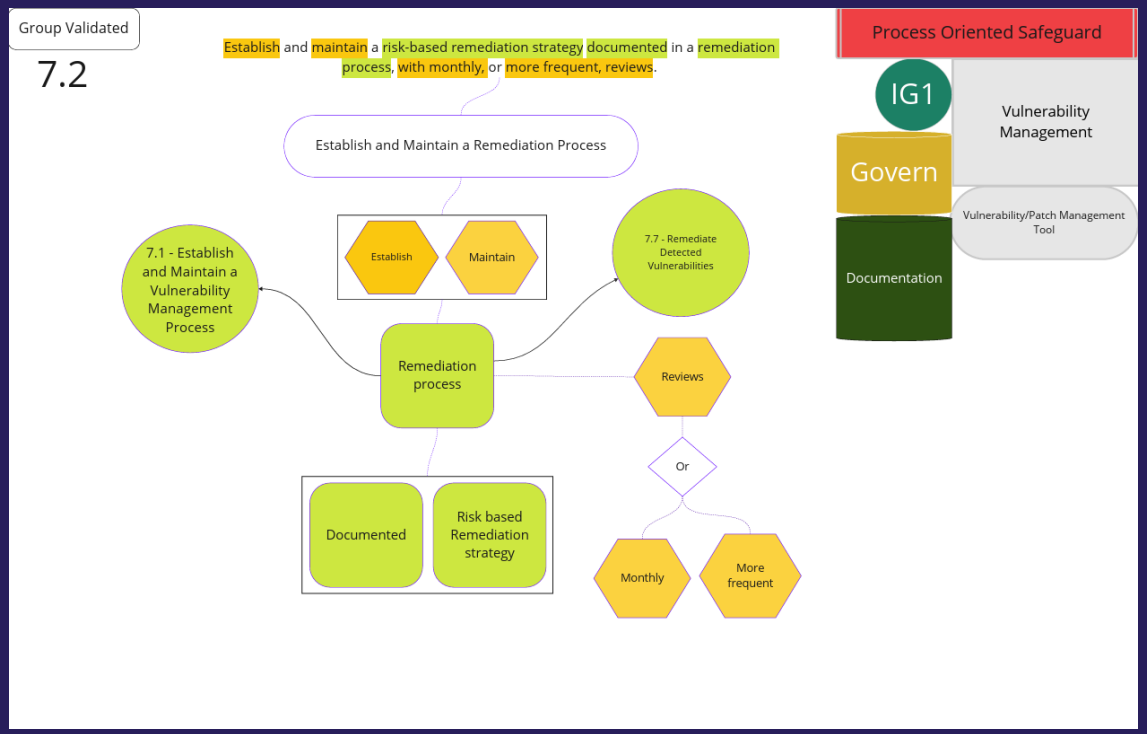


Always on, Never needs Human Interaction.....

CONTROL 7
Continuous Vulnerability Management

Safeguards: 7	IG1: 4/7	IG2: 7/7	IG3: 7/7





CVE-2024-1709 Detail

Description

ConnectWise ScreenConnect 23.9.7 and prior are affected by an Authentication Bypass Using an Alternate Path or Channel vulnerability, which may allow an attacker direct access to confidential information or critical systems.

Metrics

CVSS Version 4.0 | CVSS Version 3.x | CVSS Version 2.0

NVD enrichment efforts reference publicly available information to associate vector strings. CVSS informa… other sources is also displayed.

CVSS 3.x Severity and Vector Strings:

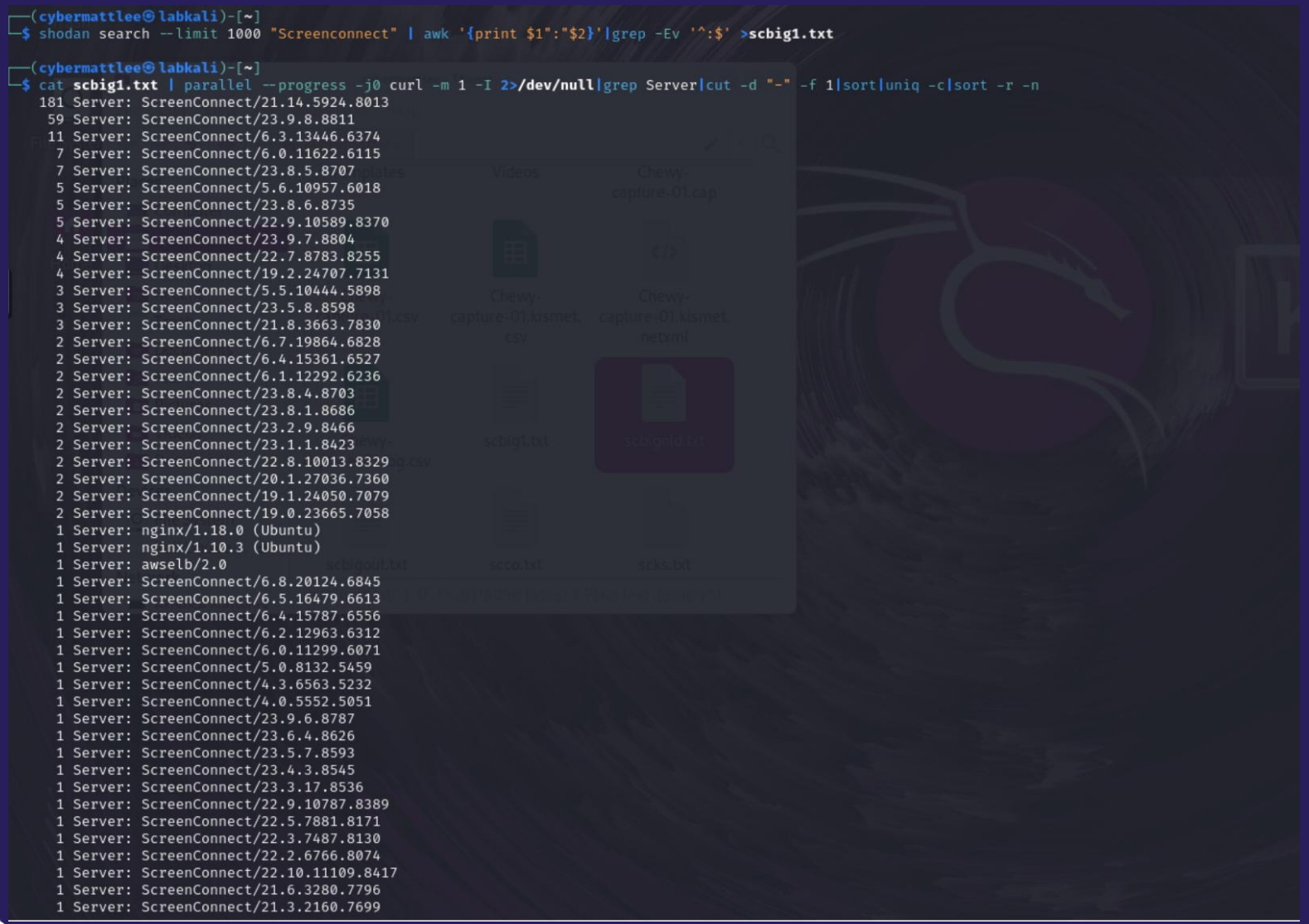
CNA: Cybersecurity and Infrastructure Security Agency (CISA) U.S. Civilian Government

Base Score: 10.0 CRITICAL

Vector: CVSS:3.1/AV:N/AC:L/PR:N/… H/A:H

A "Perfect" 10

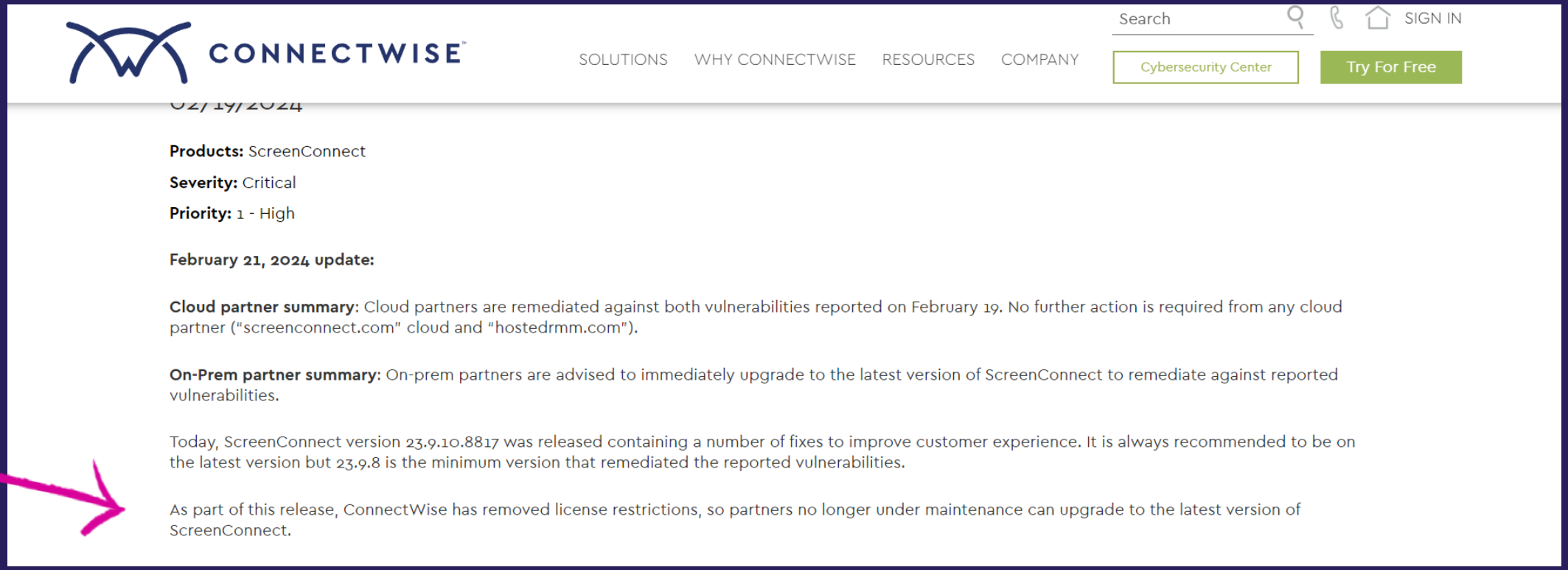
59 patched / 455 alive = 13.00% (of 1000 in a Shodan sample)
3 days after patch (morning)



```
┌──(cybermattlee㉿labkali)-[~]
└─$ shodan search --limit 1000 "Screenconnect" | awk '{print $1":"$2}'|grep -Ev '^:$' >scbig1.txt

┌──(cybermattlee㉿labkali)-[~]
└─$ cat scbig1.txt | parallel --progress -j0 curl -m 1 -I 2>/dev/null|grep Server|cut -d "-" -f 1|sort|uniq -c|sort -r -n
 181 Server: ScreenConnect/21.14.5924.8013
  59 Server: ScreenConnect/23.9.8.8811
  11 Server: ScreenConnect/6.3.13446.6374
   7 Server: ScreenConnect/6.0.11622.6115
   7 Server: ScreenConnect/23.8.5.8707
   5 Server: ScreenConnect/5.6.10957.6018
   5 Server: ScreenConnect/23.8.6.8735
   5 Server: ScreenConnect/22.9.10589.8370
   4 Server: ScreenConnect/23.9.7.8804
   4 Server: ScreenConnect/22.7.8783.8255
   4 Server: ScreenConnect/19.2.24707.7131
   3 Server: ScreenConnect/5.5.10444.5898
   3 Server: ScreenConnect/23.5.8.8598
   3 Server: ScreenConnect/21.8.3663.7830
   2 Server: ScreenConnect/6.7.19864.6828
   2 Server: ScreenConnect/6.4.15361.6527
   2 Server: ScreenConnect/6.1.12292.6236
   2 Server: ScreenConnect/23.8.4.8703
   2 Server: ScreenConnect/23.8.1.8686
   2 Server: ScreenConnect/23.2.9.8466
   2 Server: ScreenConnect/23.1.1.8423
   2 Server: ScreenConnect/22.8.10013.8329
   2 Server: ScreenConnect/20.1.27036.7360
   2 Server: ScreenConnect/19.1.24050.7079
   2 Server: ScreenConnect/19.0.23665.7058
   1 Server: nginx/1.18.0 (Ubuntu)
   1 Server: nginx/1.10.3 (Ubuntu)
   1 Server: awselb/2.0
   1 Server: ScreenConnect/6.8.20124.6845
   1 Server: ScreenConnect/6.5.16479.6613
   1 Server: ScreenConnect/6.4.15787.6556
   1 Server: ScreenConnect/6.2.12963.6312
   1 Server: ScreenConnect/6.0.11299.6071
   1 Server: ScreenConnect/5.0.8132.5459
   1 Server: ScreenConnect/4.3.6563.5232
   1 Server: ScreenConnect/4.0.5552.5051
   1 Server: ScreenConnect/23.9.6.8787
   1 Server: ScreenConnect/23.6.4.8626
   1 Server: ScreenConnect/23.5.7.8593
   1 Server: ScreenConnect/23.4.3.8545
   1 Server: ScreenConnect/23.3.17.8536
   1 Server: ScreenConnect/22.9.10787.8389
   1 Server: ScreenConnect/22.5.7881.8171
   1 Server: ScreenConnect/22.3.7487.8130
   1 Server: ScreenConnect/22.2.6766.8074
   1 Server: ScreenConnect/22.10.11109.8417
   1 Server: ScreenConnect/21.6.3280.7796
   1 Server: ScreenConnect/21.3.2160.7699
```

3 Days after the patch – CW does something Historical



CONNECTWISE

Search SIGN IN

SOLUTIONS WHY CONNECTWISE RESOURCES COMPANY Cybersecurity Center Try For Free

02/19/2024

Products: ScreenConnect

Severity: Critical

Priority: 1 - High

February 21, 2024 update:

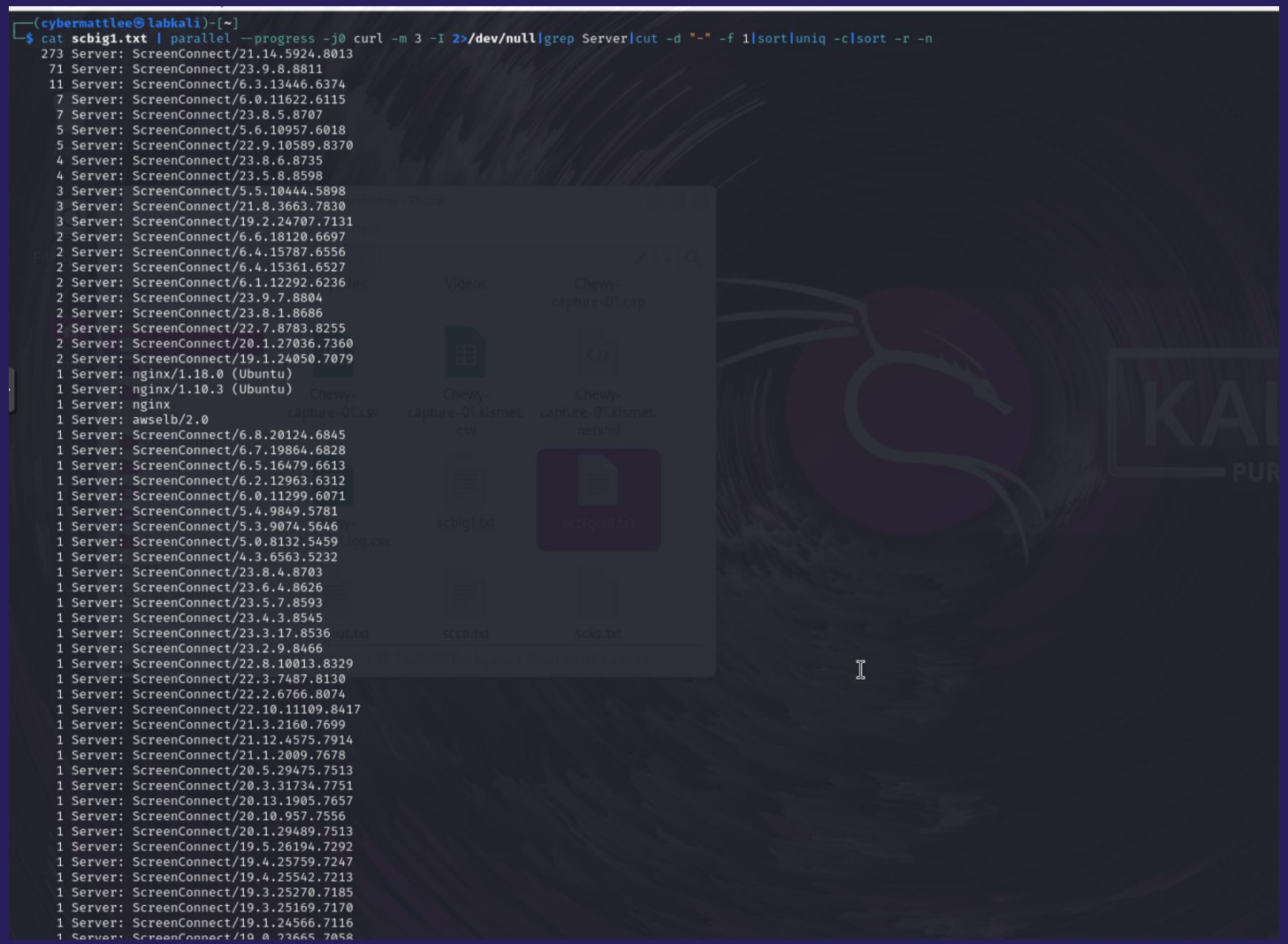
Cloud partner summary: Cloud partners are remediated against both vulnerabilities reported on February 19. No further action is required from any cloud partner ("screenconnect.com" cloud and "hostedrmm.com").

On-Prem partner summary: On-prem partners are advised to immediately upgrade to the latest version of ScreenConnect to remediate against reported vulnerabilities.

Today, ScreenConnect version 23.9.10.8817 was released containing a number of fixes to improve customer experience. It is always recommended to be on the latest version but 23.9.8 is the minimum version that remediated the reported vulnerabilities.

As part of this release, ConnectWise has removed license restrictions, so partners no longer under maintenance can upgrade to the latest version of ScreenConnect.

71 patched / 455 alive = 15.60% (of 1000 in a Shodan sample)
3 days after patch (evening)



```
┌──(cybermattlee㉿labkali)-[~]
└─$ cat scbig1.txt | parallel --progress -j0 curl -m 3 -I 2>/dev/null|grep Server|cut -d "-" -f 1|sort|uniq -c|sort -r -n
    273 Server: ScreenConnect/21.14.5924.8013
     71 Server: ScreenConnect/23.9.8.8811
     11 Server: ScreenConnect/6.3.13446.6374
      7 Server: ScreenConnect/6.0.11622.6115
      7 Server: ScreenConnect/23.8.5.8707
      5 Server: ScreenConnect/5.6.10957.6018
      5 Server: ScreenConnect/22.9.10589.8370
      4 Server: ScreenConnect/23.8.6.8735
      4 Server: ScreenConnect/23.5.8.8598
      3 Server: ScreenConnect/5.5.10444.5898
      3 Server: ScreenConnect/21.8.3663.7830
      3 Server: ScreenConnect/19.2.24707.7131
      2 Server: ScreenConnect/6.6.18120.6697
      2 Server: ScreenConnect/6.4.15787.6556
      2 Server: ScreenConnect/6.4.15361.6527
      2 Server: ScreenConnect/6.1.12292.6236
      2 Server: ScreenConnect/23.9.7.8804
      2 Server: ScreenConnect/23.8.1.8686
      2 Server: ScreenConnect/22.7.8783.8255
      2 Server: ScreenConnect/20.1.27036.7360
      2 Server: ScreenConnect/19.1.24050.7079
      1 Server: nginx/1.18.0 (Ubuntu)
      1 Server: nginx/1.10.3 (Ubuntu)
      1 Server: nginx
      1 Server: awselb/2.0
      1 Server: ScreenConnect/6.8.20124.6845
      1 Server: ScreenConnect/6.7.19864.6828
      1 Server: ScreenConnect/6.5.16479.6613
      1 Server: ScreenConnect/6.2.12963.6312
      1 Server: ScreenConnect/6.0.11299.6071
      1 Server: ScreenConnect/5.4.9849.5781
      1 Server: ScreenConnect/5.3.9074.5646
      1 Server: ScreenConnect/5.0.8132.5459
      1 Server: ScreenConnect/4.3.6563.5232
      1 Server: ScreenConnect/23.8.4.8703
      1 Server: ScreenConnect/23.6.4.8626
      1 Server: ScreenConnect/23.5.7.8593
      1 Server: ScreenConnect/23.4.3.8545
      1 Server: ScreenConnect/23.3.17.8536
      1 Server: ScreenConnect/23.2.9.8466
      1 Server: ScreenConnect/22.8.10013.8329
      1 Server: ScreenConnect/22.3.7487.8130
      1 Server: ScreenConnect/22.2.6766.8074
      1 Server: ScreenConnect/22.10.11109.8417
      1 Server: ScreenConnect/21.3.2160.7699
      1 Server: ScreenConnect/21.12.4575.7914
      1 Server: ScreenConnect/21.1.2009.7678
      1 Server: ScreenConnect/20.5.29475.7513
      1 Server: ScreenConnect/20.3.31734.7751
      1 Server: ScreenConnect/20.13.1905.7657
      1 Server: ScreenConnect/20.10.957.7556
      1 Server: ScreenConnect/20.1.29489.7513
      1 Server: ScreenConnect/19.5.26194.7292
      1 Server: ScreenConnect/19.4.25759.7247
      1 Server: ScreenConnect/19.4.25542.7213
      1 Server: ScreenConnect/19.3.25270.7185
      1 Server: ScreenConnect/19.3.25169.7170
      1 Server: ScreenConnect/19.1.24566.7116
      1 Server: ScreenConnect/19.0.23665.7058
```

90 patched / 419 alive = 21.48% (of 1000 in a Shodan sample)
4 days after patch AND 1 day after a FREE upgrade

```
┌──(cybermattlee㉿labkali)-[~]
└─$ cat scbig1.txt | parallel --progress -j0 curl -m 4 -I 2>/dev/null|grep Server|cut -d "-" -f 1|sort|uniq -c|sort -r -n
    242 Server: ScreenConnect/21.14.5924.8013
     68 Server: ScreenConnect/23.9.8.8811
     22 Server: ScreenConnect/23.9.10.8817
     11 Server: ScreenConnect/6.3.13446.6374
      8 Server: ScreenConnect/6.0.11622.6115
      5 Server: ScreenConnect/5.6.10957.6018
      5 Server: ScreenConnect/5.5.10444.5898
      4 Server: ScreenConnect/23.8.5.8707
      4 Server: ScreenConnect/22.9.10589.8370
      2 Server: ScreenConnect/6.6.18120.6697
      2 Server: ScreenConnect/6.4.15787.6556
      2 Server: ScreenConnect/6.4.15361.6527
      2 Server: ScreenConnect/23.8.6.8735
      2 Server: ScreenConnect/23.5.8.8598
      2 Server: ScreenConnect/22.7.8783.8255
      2 Server: ScreenConnect/20.1.27036.7360
      2 Server: ScreenConnect/19.2.24707.7131
      1 Server: nginx/1.18.0 (Ubuntu)
      1 Server: nginx/1.10.3 (Ubuntu)
      1 Server: nginx
      1 Server: awselb/2.0
      1 Server: ScreenConnect/6.5.16479.6613
      1 Server: ScreenConnect/6.2.12963.6312
      1 Server: ScreenConnect/6.1.12292.6236
      1 Server: ScreenConnect/6.0.11299.6071
      1 Server: ScreenConnect/5.3.9074.5646
      1 Server: ScreenConnect/5.0.8132.5459
      1 Server: ScreenConnect/4.3.6563.5232
      1 Server: ScreenConnect/23.9.7.8804
      1 Server: ScreenConnect/23.8.1.8686
      1 Server: ScreenConnect/23.5.9.8811
      1 Server: ScreenConnect/23.5.7.8593
      1 Server: ScreenConnect/23.3.17.8536
      1 Server: ScreenConnect/23.2.9.8466
      1 Server: ScreenConnect/22.8.10013.8329
      1 Server: ScreenConnect/22.2.6766.8074
      1 Server: ScreenConnect/21.3.2160.7699
      1 Server: ScreenConnect/20.3.31734.7751
      1 Server: ScreenConnect/20.13.1905.7657
      1 Server: ScreenConnect/20.10.957.7556
      1 Server: ScreenConnect/19.4.25759.7247
      1 Server: ScreenConnect/19.4.25542.7213
      1 Server: ScreenConnect/19.3.25169.7170
```

Afternoon!

I have a client that's running an old DOS program that needs to be run on Windows 7. His office 365 package has updated and broken, because I'm guessing it's know longer compatable. Has anyone got a workaround for 365 on Windows 7?

Much appreciated in advance.

Just curious: The other day, I installed a fresh Windows 7 off a CD for a client. One wrinkle was that I could not activate the license. When Microsoft says they no longer support WIN7, that doesn't mean they stopped activating licenses. Right? Maybe I just need to buy a new key?

My company has been using Threatlocker for a couple of months. We included ringfencing. We have not elected to have a spam filter/email protection app yet because theatlocker protects against any script, powershell, command line or other malicious attempts to change apps or OS. If we have that protection, do we need spam and email security? If user clicks link that attempts to change their computer in any way, stopped by TL. Only way is a password reset link which if they did get password, 2fa would stop that and notify us. I'm not convinced we NEED email protection. Any input is welcome. Thank you all in advance.

I have been holding off posting trying to find a solution with no success. I have a small school district ruining server 2012r2. Fully updated, etc, etc.
The issue is that the print spooler service keeps going from automatic to disabled. 30 seconds to remote in and fix it, but it happens daily or multiple times a day.
Anyone have any clue what might be the cause/ fix? I am willing to try literally anything.
TIA.

Fictitious Kill Chain Case Study

"This Fictitious Kill Chain Case Study is as real as a SOC analyst's full lunch break—**purely hypothetical**.

Any resemblance to actual organizations and/or events is purely coincidental, not actionable, and absolutely not the basis for a compliance audit or legal inquiry."

4.T™ ENGINEERING

CASE STUDY

Introducing 4TEs Managed Services Provider (MSP)

Robert "Guy" Fleegelman, President FleegTech

Robert "Guy" Fleegman's quest began in the galaxy of Hollywood, where he cut his teeth managing IT for film studios, convention centers, and scrappy production startups. But after seeing too many **bad IT fixes take down mission-critical systems**, he set out on his own, founding **FleegTech Managed Services** in 2004.

Bridging IT and Operational Technology (OT), FleegTech helps **manufacturers, robotics startups, and industrial tech firms** secure their networks **without breaking production environments.** Guy's team specializes in **scalable cloud-first IT solutions** that let businesses innovate without disruption.

"Great IT isn't just about keeping systems running—it's about knowing the plumbing and what's running beneath the surface before it's too late."

-Guy Fleegelman

FLEEGTECH
MANAGED SERVICES

The Kill Chain

Crypto Miner Compromised VDI Performance:

A common crypto miner evaded anti-malware controls and caused high resource usage over the weekend, significantly slowing down the VDI environment and preventing 4TE developers from working.

Assumed Monitoring Responsibilities Led to Oversight:

4TE assumed the MSP was monitoring system performance, but the MSP was only tasked with security, not performance monitoring. CSP performance alerts were never set up, and no threshold was defined for declaring performance incidents.

Delayed Incident Detection Due to Lack of Reporting:

No 4TE employees reported the slowdown or process failures for over a week, and the MSP identified the issue only after reviewing 7 days of performance logs following the reported outage.

The Kill Chain

Firmware Update Compromised Controller Communication:

A routine DNS change in a firmware update, pushed via the CI/CD pipeline, inadvertently redirected chemical controllers to a **server controlled by a Threat Actor (TA)**. The TA hijacked the command-and-control infrastructure, causing uncontrolled chemical releases across 10,000 cities.

Widespread Impact and Imminent Threat:

Chemical overflows occurred randomly, leading to a critical public safety risk. The TA demanded a ransom with a 12-hour deadline, threatening full-volume chemical dumps. The issue has escalated to CISA due to its national security implications.

The Kill Chain

Federal Agencies Involved – No Logs and Finger pointing:

After the TA hijacked the command-and-control infrastructure, causing uncontrolled chemical releases across 10,000 cities CISA and other law enforcement get involved. FleegTech nor 4TE were found to have any meaningful logs, hampering incident containment and response efforts.

4TE Left Responsible for....

Cascading lapses in accountability come to light after catastrophic consequences across the country. Prolonged disruption to safe water supply, countless hours of remediation, and potentially unrecoverable reputational loss for 4TE. Who is ultimately responsible? Who will be held to account?

RSAC 2025 Conference

SRM 4TE 4TW

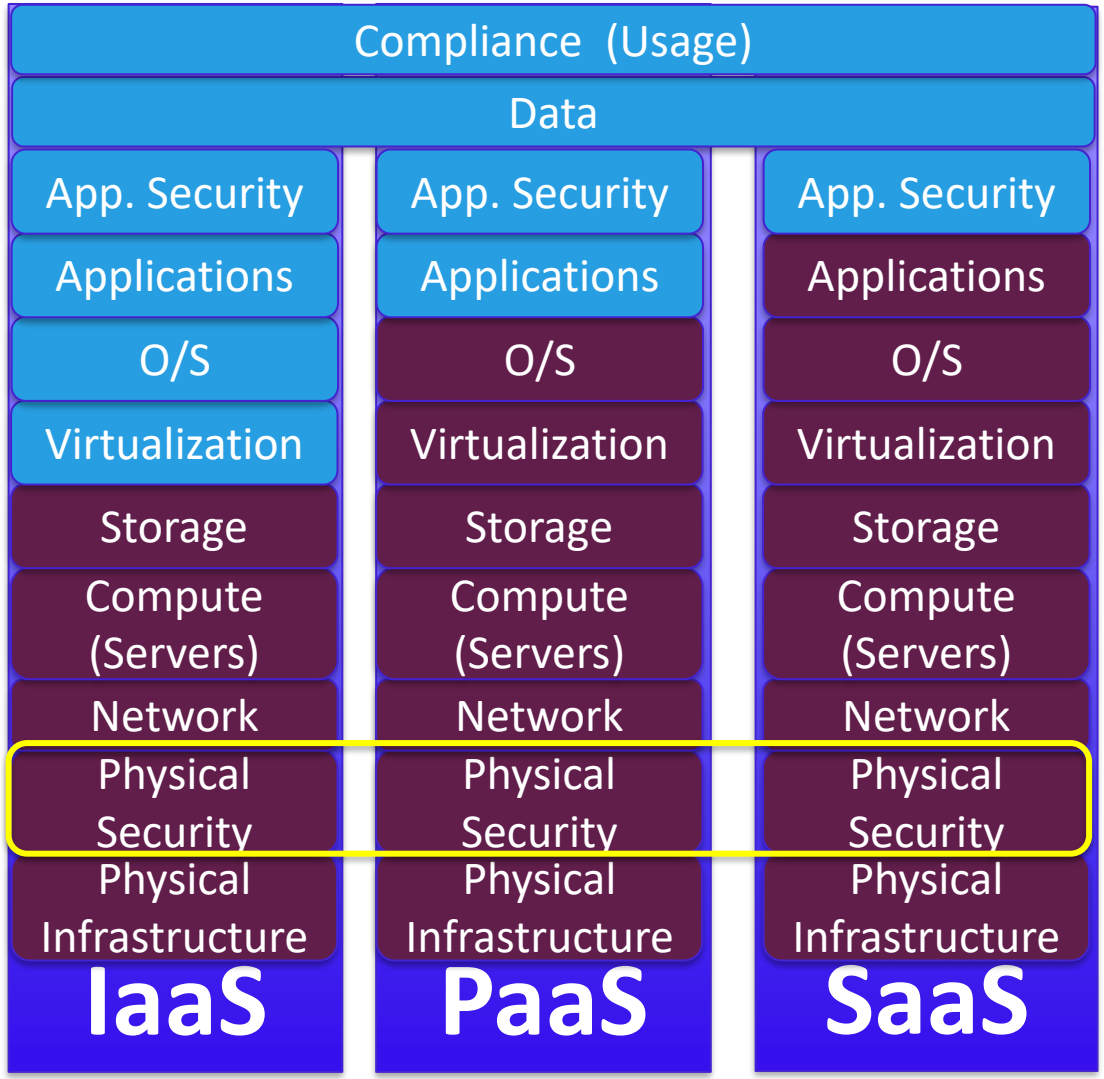
Insight from Incident

Many Voices.
One Community.

Shared Responsibility Matrix

- Shared Responsibility Models | Matrices (SRMs) are not new
- SRMs long-critical in Cloud Computing
- More ecosystem partners → More important they are
- SRMs are not 1:1, but 1:*many*
- The system owner is ultimately responsible for full system compliance

Shared Responsibility Matrix

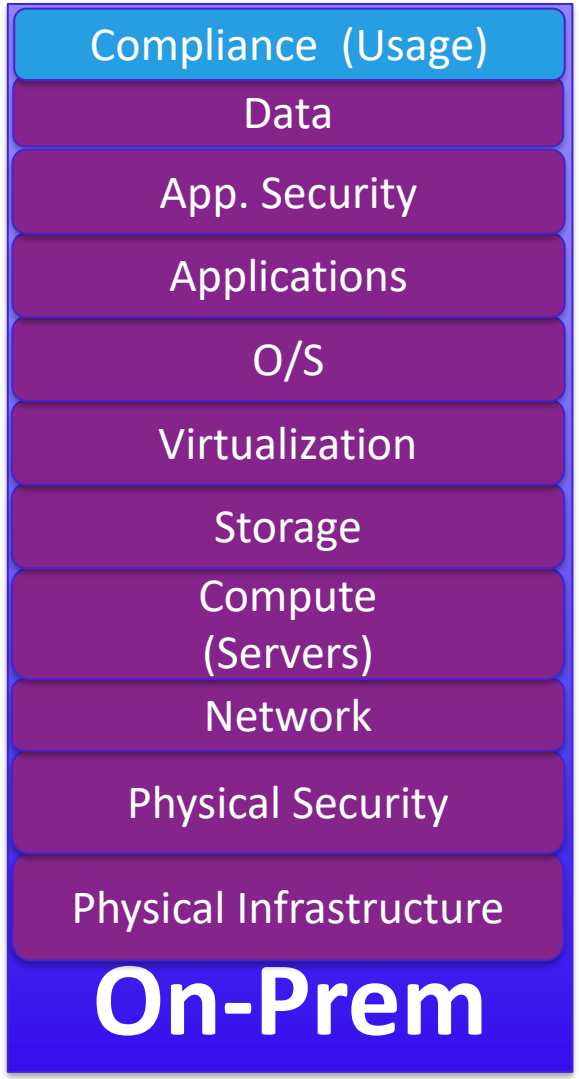


Things you are responsible for

Things the service provider is responsible for

Cloudy Services

Shared Responsibility Matrix



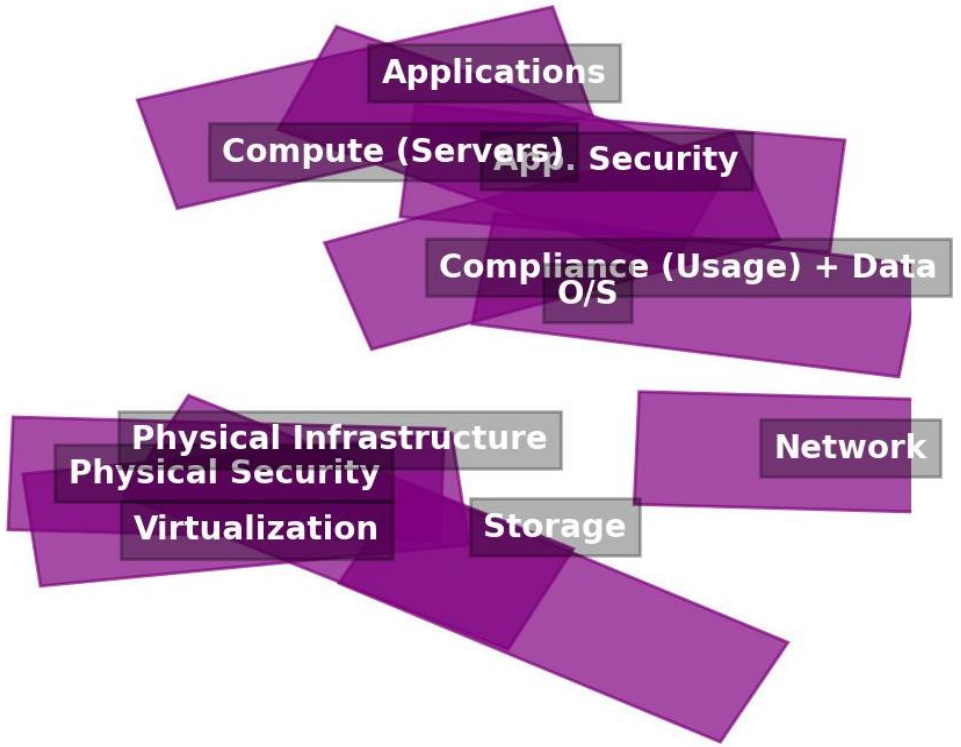
Things you are responsible for

Things the service provider **might be** responsible for

Hybrid / On-Prem Services

Key Elements of a Shared Responsibility Model

An SRM should clearly identify who is responsible (for what) when:



Key Elements of a Shared Responsibility Model

What does "Good" Look like? **A.N.C.H.O.R**

- **A - Agreed Metrics:** *Agreed Methods of Measurement*
  - Define measurable success/failure criteria.
- **N - Named Scope:** *Clearly identifies scope of (eco)system and controls*
  - Know exactly what is—and isn't—in scope.
- **C - Clear Responsibilities:** *Clear responsibility, including legal transference of risk*
  - Document who owns what, including legal language.
- **H - Handled Data:** *Understanding of the in-scope information and applicable safe handling*
  - Define the data types, custody requirements, and protections.
- **O - Operational Specifics:** *Identifies specifics (e.g. log retention)*
  - Detail configurations, durations, and control precision.
- **R - Risks Identified:** *Not glossing over potential risks, reporting requirements, and definitions*
  - Be transparent about important language, requirements, residual and transferred risks.

Key Elements of a Shared Responsibility Model

Simplistic Considerations

- What defines an incident?
- What logs are required to be retained?
- Who arbitrates disagreements (before lawyers get involved)?
- What rights does each party have over system changes?

- **Who Reports incident(s) to whom?**

Key Elements of a Shared Responsibility Model

BACKGROUND: WHAT IS CIRCIA?

Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA)

The Nation's Cyber Defense Agency

CompTIA ChannelCon

JULY 30 – AUGUST 1, 2024 | ATLANTA

#ChannelCon

8

SRMs aren't just for IT

Fue

by SBG

Firefighte

Ransomw encryptio

'Codefinger' crims

Jessica Lyons

A new ransomware crew cloud giant's own server victims' data before dem required to decrypt it.

Halcyon threat hunters s recent weeks observed t whom were AWS native

Codefinger breaks into v compromised AWS keys and "`s3:PutObject`" req

AutoNation: CDK Hack Will Hurt Earnings

BY **PYMNTS** | JULY 15, 2024

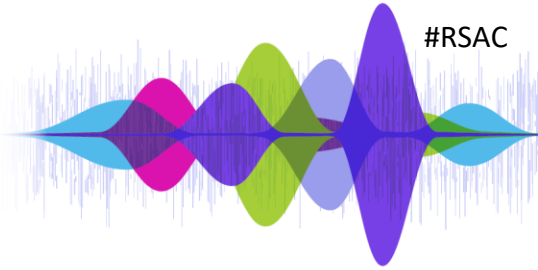
The impact of the hack on car dealership software firm CDK Global continues to reverberate.

AutoNation, one of the largest dealership chains in the country, warned on Monday (July 15) that the cyberattack will impact its second quarter earnings by $1.50 per share. The company said in a Securities and Exchange Commission (SEC) filing that while some systems have been restored, it is still dealing with the fallout of the hack.

From Kill Chain to Clarity

When "Someone" is Responsible, No One Is — Until Now

From Kill Chain to Clarity



Dissecting the Kill Chain:

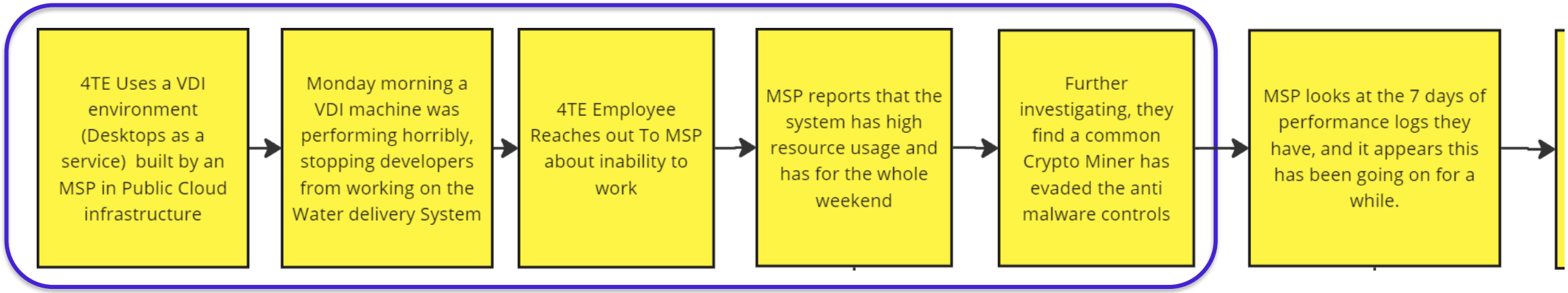
- Identify (all of) the players
- Identify their roles
- Identify their responsibility
- Examine what went wrong

…let’s gain some insight from their incident

From Kill Chain to Clarity

Who	Role
4TE Board of Directors	Risk Tolerance, Oversight, Resource Allocation
4TE Executive Leadership	Executing on the board's directives, informing board of risk, operating the company, choosing ecosystem partners, creating and approving policy
4TE IT Leadership	Technology platform management, resource management, tactical policy enforcement
4TE Technical Staff	Code Development, Secure Coding Practices, Secure CI/CD
FleegTech	IT MSP Supporting 4TE, VDI, Productivity Tenant Management, VDI/System Security

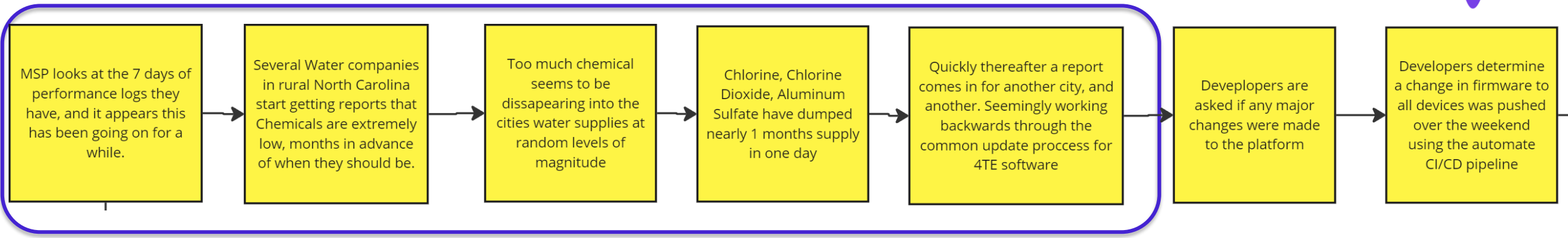
From Kill Chain to Clarity


4TE Uses a VDI environment (Desktops as a service) built by an MSP in Public Cloud infrastructure
Monday morning a VDI machine was performing horribly, stopping developers from working on the Water delivery System
4TE Employee Reaches out To MSP about inability to work
MSP reports that the system has high resource usage and has for the whole weekend
Further investigating, they find a common Crypto Miner has evaded the anti malware controls
MSP looks at the 7 days of performance logs they have, and it appears this has been going on for a while.

Early-Stage Kill Chain

- No shared definition of what constitutes an incident (CIS 17)
- No defined End User training or reporting requirement (CIS 14)
- No shared / coordinated incident response procedure between FleegTech and 4TE
- 4TEs IT Leadership and Executives disagree on materiality of crypto miner – is this an incident?

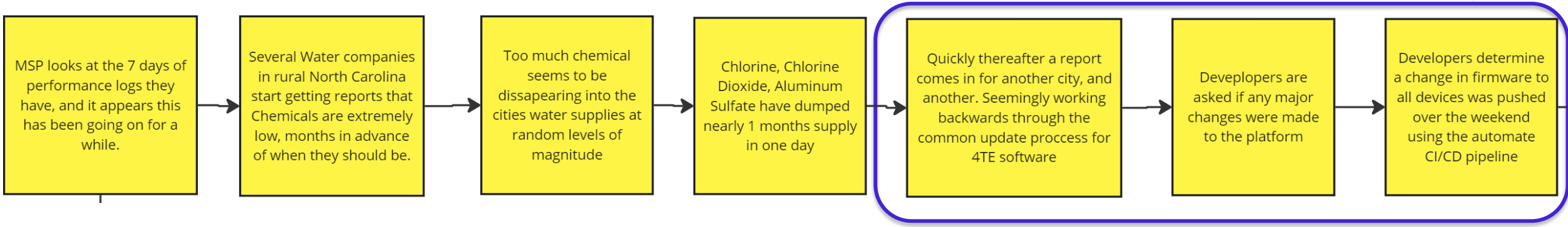
From Kill Chain to Clarity


MSP looks at the 7 days of performance logs they have, and it appears this has been going on for a while.
Several Water companies in rural North Carolina start getting reports that Chemicals are extremely low, months in advance of when they should be.
Too much chemical seems to be dissapearing into the cities water supplies at random levels of magnitude
Chlorine, Chlorine Dioxide, Aluminum Sulfate have dumped nearly 1 months supply in one day
Quickly thereafter a report comes in for another city, and another. Seemingly working backwards through the common update proccess for 4TE software
Deveplopers are asked if any major changes were made to the platform
Developers determine a change in firmware to all devices was pushed over the weekend using the automate CI/CD pipeline

Mid-Stage Kill Chain

- MSP has limited logs (7 days) "because they weren't required to have any more"
- Developers aren't using a change-control process (They don't know what changes are legitimate)
- 4TE learns of two new (unknown) persistent access methods that were implemented by MSP – unsure if they are contributory to incident

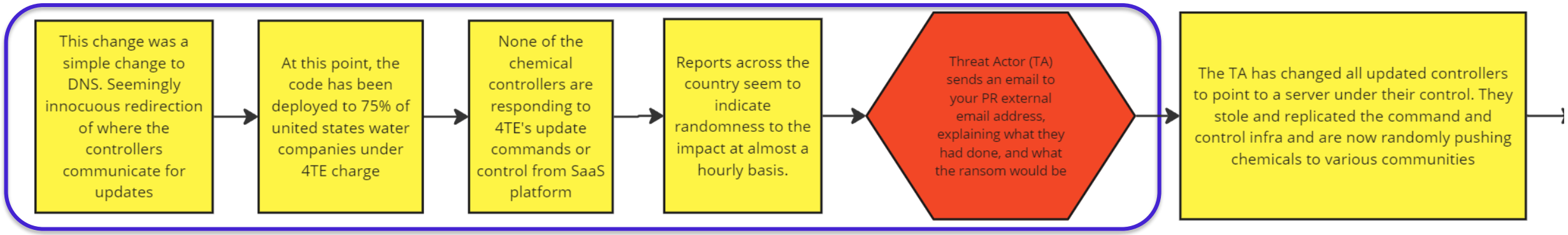
From Kill Chain to Clarity


MSP looks at the 7 days of performance logs they have, and it appears this has been going on for a while.
Several Water companies in rural North Carolina start getting reports that Chemicals are extremely low, months in advance of when they should be.
Too much chemical seems to be dissapearing into the cities water supplies at random levels of magnitude
Chlorine, Chlorine Dioxide, Aluminum Sulfate have dumped nearly 1 months supply in one day
Quickly thereafter a report comes in for another city, and another. Seemingly working backwards through the common update proccess for 4TE software
Deveplopers are asked if any major changes were made to the platform
Developers determine a change in firmware to all devices was pushed over the weekend using the automate CI/CD pipeline

Mid-Stage Kill Chain

- No defined requirement by 4TE for logging granularity, configuration, or retention
- MSP learns of CI/CD platform and 4TEs expectation that they are monitoring/securing it
- CI/CD platform is cloud-based and doesn't record events for more than 7 days.
- MSP and 4TE Board are not aware of this platform's configuration; Violates regulatory requirements

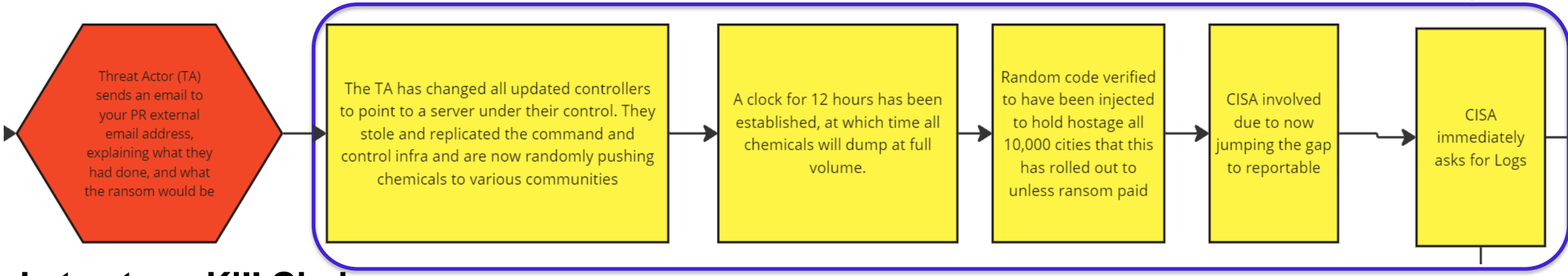
From Kill Chain to Clarity


This change was a simple change to DNS. Seemingly innocuous redirection of where the controllers communicate for updates
At this point, the code has been deployed to 75% of united states water companies under 4TE charge
None of the chemical controllers are responding to 4TE's update commands or control from SaaS platform
Reports across the country seem to indicate randomness to the impact at almost a hourly basis.
Threat Actor (TA) sends an email to your PR external email address, explaining what they had done, and what the ransom would be
The TA has changed all updated controllers to point to a server under their control. They stole and replicated the command and control infra and are now randomly pushing chemicals to various communities

Mid-late stage Kill Chain

- Chaos ensues as MSP provides 4TE service tickets showing unsanctioned security changes "performed as requested" (requested by a developer); Changes never reported to 4TE IT leadership
- These changes possibly contributory to incident?
- MSP implemented their "best practices" for many system configurations
- These "best practices" found to be sub-par to 4TEs presumed standards and requirements

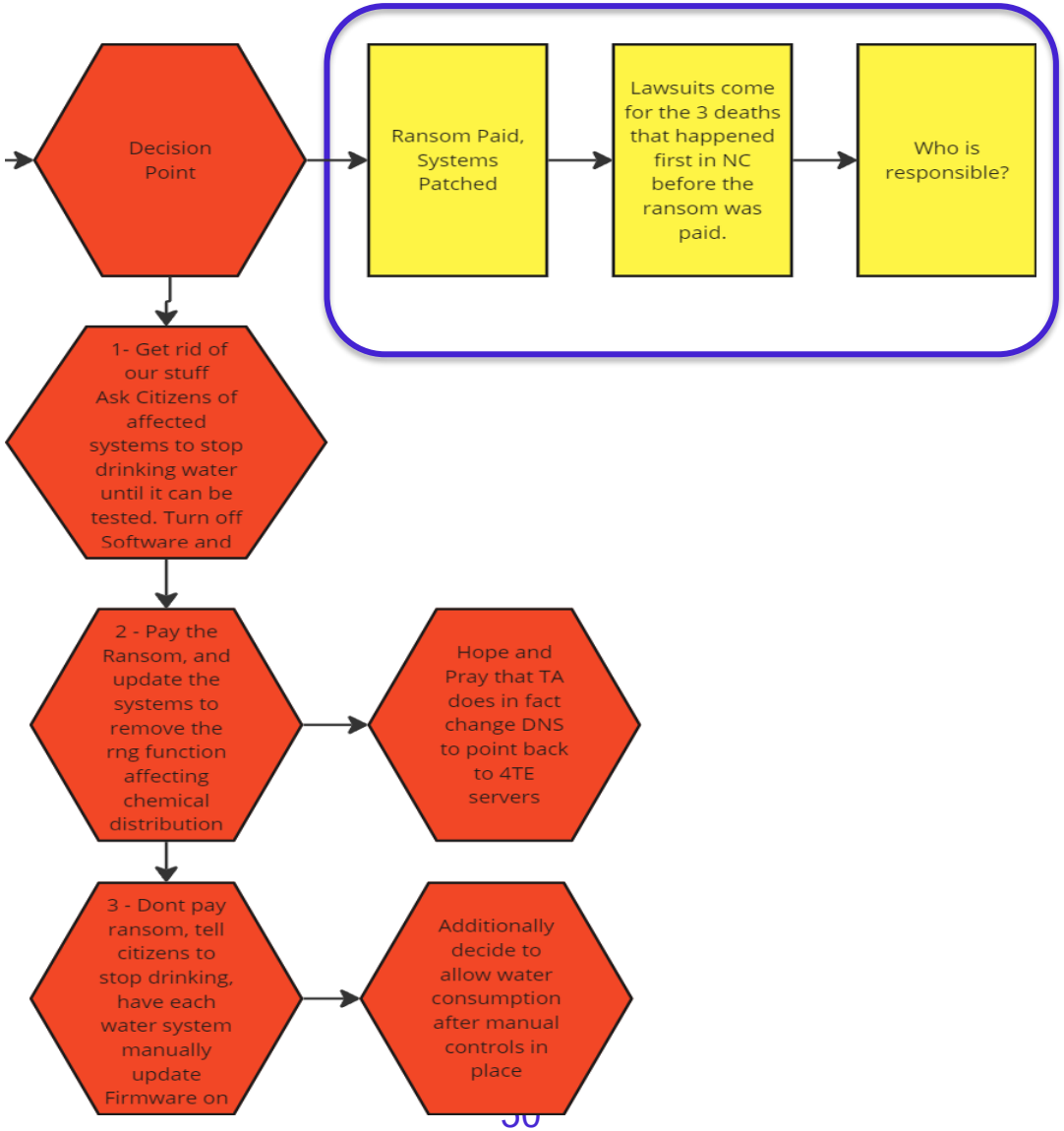
From Kill Chain to Clarity


Threat Actor (TA) sends an email to your PR external email address, explaining what they had done, and what the ransom would be
The TA has changed all updated controllers to point to a server under their control. They stole and replicated the command and control infra and are now randomly pushing chemicals to various communities
A clock for 12 hours has been established, at which time all chemicals will dump at full volume.
Random code verified to have been injected to hold hostage all 10,000 cities that this has rolled out to unless ransom paid
CISA involved due to now jumping the gap to reportable
CISA immediately asks for Logs

Late stage Kill Chain

- Scope and Scale of event deemed a reportable incident by 4TEs board
- FleegTech learns they have reporting obligation when 4TEs lawyers inform them
- Government Agencies are involved & request logs; Few-to-None Exist
- MSP is singled out – points to contract clause stating they didn't "do" compliance
- Board attested to the cybersecurity and data security posture of 4TE in regulatory filings

From Kill Chain to Clarity


Decision Point
Ransom Paid, Systems Patched
Lawsuits come for the 3 deaths that happened first in NC before the ransom was paid.
Who is responsible?
1- Get rid of our stuff Ask Citizens of affected systems to stop drinking water until it can be tested. Turn off Software and
2 - Pay the Ransom, and update the systems to remove the rng function affecting chemical distribution
Hope and Pray that TA does in fact change DNS to point back to 4TE servers
3 - Dont pay ransom, tell citizens to stop drinking, have each water system manually update Firmware on
Additionally decide to allow water consumption after manual controls in place

From Kill Chain to Clarity

- SRM with FleegTech should:
  - Clearly specify the scope of systems and services
  - Include roles, rights, and reporting/review of the same
  - Define required end-user training (4TE)
  - Identify minimum levels of operational continuity requirements

From Kill Chain to Clarity

- SRM with FleegTech should:
  - Specify mutual recordkeeping requirements
  - Identify the bounds of responsibility for each organization
  - Define escalation paths and inter-organization communications
  - Clearly control how changes to service(s) are handled, communicated, and approved

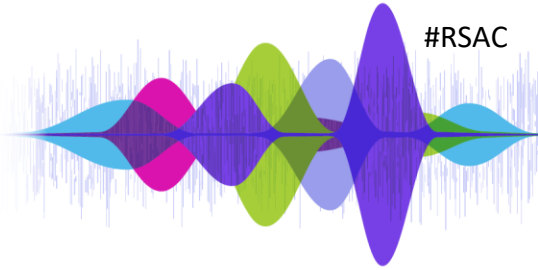
From Kill Chain to Clarity

- SRM with FleegTech should:
  - Detail how key metrics are tracked, recorded, and responded
  - Define 4TEs regulatory requirements, clearly and understandably
  - Contain requirement for mutual Incident Response Plans (IRPs)
  - Contain definition of "Incidents" and how IRPs cooperate/align

From Kill Chain to Clarity

- SRM with FleegTech should:
  - Incorporate specific legal/regulatory requirements (practice level)
  - Identify specific security frameworks to be applied (e.g. CIS)
  - Identify specific security standards (e.g. CISA CPGs)
  - Clearly assign accountability for technical, tactical, and governance
  - Be written in mutually understandable language

From Kill Chain to Clarity



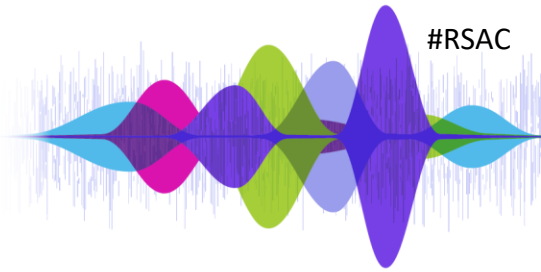
Dissecting the Kill Chain:

- SRM with FleegTech should:
  - Define specific risk transference requirements
  - Define minimum risk transference capacity
  - **A.N.C.H.O.R** the fundamentals of the service relationship

Making Application

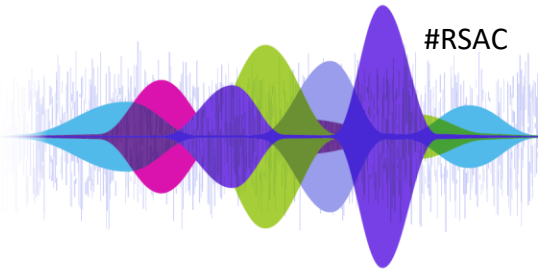
Insight Through Incident

Making Application



- SRMs have long been in-place within the cloud computing industry
- Complex Multi-Vendor ecosystems are increasingly normal
- Third parties (MSPs, CSPs, etc.) responsibilities' all must be coordinated and communicated
- SMBs (and their MSPs) complicate and impose risk to supply chains
- Non-cloud native environments demand equal consideration as cloud

Making Application



- **When you return:**
  - For larger organizations:
    - Evaluate your SMB suppliers and the SRMs you have in place with them
    - Empower your supply chain!
      - Many of these organizations operate below the "cyber poverty level"
      - What can you do to assist them? Educate them to develop SRMs in their ecosystem
    - Complex Multi-Cloud ecosystems demand oversight – who's watching, reviewing?
    - Evaluate your SRMs, beginning with those handling the most operationally critical information
    - Do SRMs align with compliance requirements? Reporting Requirements?

Making Application

- **When you return:**
  - For smaller organizations:
    - Consider the cybersecurity framework you are using...
    - Evaluate your ecosystem and the SRMs in place today...
      - Do the two align? Who is regularly reviewing this?
    - A cloud service may be 'capable' of a thing, but it likely requires advance configuration. Verify!
    - Can FleegTech exist within your ecosystem?
    - Do SRMs align with compliance requirements? Reporting Requirements?
    - Are the SRMs clear – **to a practice level** – of who is responsible for what?

Making Application

- **When you return:**
  - For all organizations
    - The "Incident" experiment.
      - At the board or executive level – ask

"What cybersecurity incident must we know about and memorialize"

      - Consult SRMs with Critical Ecosystem Partners and Downstream Vendors
        - Ask the same question:

"What cybersecurity incidents would you inform us about and how?"

Making Application

Shared Responsibility is like a dance—if everyone assumes *someone* else is leading, no one moves, and the whole thing dissolves into an awkward shuffle of confusion and blame. In a modern cloud-enabled business, security, compliance, and resilience aren't just the provider's gig or the customer's solo; they're a synchronized performance. Done right, it's a seamless tango. Ignored, it's a frantic game of musical chairs—where the music keeps playing, but your business might not.

"Someone's" responsibility is No-one's responsibility

RSAC™ 2025 Conference

Many Voices.
One Community.

Matt: https://www.linkedin.com/in/cybermattlee

mlee@pax8.com

Lawrence: https://www.linkedin.com/in/lawrence-cruciana/

lcruciana@corp-infotech.com